ON GERMAN DIPLOMATIC CIPHERS

Notes from an interrogation of WILHELM THOEM, of von RIBBENTROPP's personal staff.

1. The attached notes, from an F.B.I. field interrogation of WILHELM THOEM have been forwarded by Director SID ETOUSA.

2. THOEM had previously been a German Embassy employee in Mexico City (1933-1940) and Santiago(1940-1943)

3. The notes are in two parts:-

a) BLOCKVERFAHREN and

b) GRUNDVERFAHREN and appear to include THOEM's entire knowledge of German cryptographic systems. He has now been cleared for release.

TICOM
31 July 1945

No. of pages 6

Distribution

British
Director
D.D.3
D.D.4
D.D.(N.S.)
D.D.(M)
D.D.(A.S.)
A.D.(C.C.R.)(2)
Lt. Col. Leathem

U.S.
OPNAV-G(2)(via Lt. Pendergrass)
G-2(via Lt. Col. Rilles)
S.S.A.(2)(via Major Seaman)
Director, S.I.D. ETOUSA(via Lt Col. Johnson)

TICOM
Chairman
S.A.C.(2)
Cdr. Bacon
Cdr. MacKenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Cdr. Manson
Major Seaman
Lt. Bachus
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files(2)

Additional
Major G.W.Morgan.

I. "BLOCKVERFAHREN"
(CIPHER PAD-ENCODE)

1. "Deutscher Satzbuch" This is a German language code book which is used in first placing a message into a number code. It was not regarded by the German Foreign Office as being secret ("nicht geheim").F.O. missions in the English speaking countries used an "Englische Satzbuch"which similarly gave a five figure code for English words. Although not secret and not a commercial code, the "Satzbuch" was used only by the German F. O. and not by other branches of the government. In all Latin America, German embassies and consulates used the "Deutscher Satzbuch". The "Englische Satzbuch" is believed to have been used in the U.S.

2. The "Zifferblock"(cipher pad) was used in the next steps. The block consisted of 100 sheets of paper consecutively numbered from 1 to 100. Each sheet "block blatt" had printed on it 8 lines of 5 digit numbers, 6 groups per line-- a total of 48 of the 5 digit groups per page.

a. Security : The numbers on the pad were believed to be chosen on a lottery basis, but a machine was not known to have been used. The "blocks"were made up in duplicate in Berlin, where one copy was kept for decoding, while the other copy was sent to the Foreign Embassy. The pads were bound in paper, threaded with thread, the ends of which were sealed to the back of the pad. The sheets themselves were perforated and could be cut out of the pad, one at a time, with a knife. Each page was used for but one message. Used sheets were kept for one month (in Mexico and Chile) and then burned.

b. Use: Numbers on the "block" sheets were added to the message as it had come out of the "Satzbuch". The blocks were of different colors and each consulate used only one color. In Berlin this assisted in easily finding the proper pad for decoding.

3. Sample:

"und"	-	76500	(from "Satzbuch")
		89142	(from "block")
final message-		55642	(add without carrying)

Sample message from,e.g. Mexico embassy to Berlin Foreign Office:
(cable address)(msg.no.)(day of month) (block no.)(page No)
"Auswartige Berlin. 155/24 87/34
XXXXX XXXXX XXXX.....etc. (coded message)XXXX XXXX 00020"
(no. of secret groups)

Note that the group indicating "block" and page number was usually a 4 digit group--possibly always. Also if this group was followed immediately by a plain text "zwei"(two),this meant that the 2nd half of the page- the last 24 groups were being used. This was sometimes done when the supply of pads ran short.

4. Decoding

The process is obvious from the above since it only involves doing the process in reverse:

1) Proper cipher page is selected and the groups are subtracted from the message groups.
2) The results number groups which are turned into words by looking up the numbers in the "Satzbuch".

As long as the cipher pads are secret and not in unauthorized hands, the German Foreign Office felt the above code to be highly secure.

II. GRUNDVERFAHREN
("Ground"or "Basic")

This is a more complicated method of encoding which makes use of the following:

1. The Satzbuch (described above)
2. A cipher book of two types:
   a. "Tangens Tafel"(tangent table) T.T.
   b. "Grad Tafel" (degree or graduated table)G.T.
   Either or both may be used.
3. "Schlusselblock"(key pad)

This system involves:1-coding by use of the "Satzbuch ",2-making the message secure by adding numbers from the cipher books,3-including in the message an indicator as to how the cipher book was used. In the latter, the "key pad" is used.

1. "Satzbuch"
This is first used to change words and phrases into 5 digit groups as in the "Block" system.

2. Cipher books
Since two books were used, variations were possible.
a. Using only the "Tangens Tafel"(tangent table)
(This was used in Mexico City up until 1940 and possibly thereafter, according to the informant.)
Description of "TangensTafel": This is a 100 or 200(?) page book which served as a substitute for a cipher pad, i.e., it provided groups of 5 digits to be added to the "satzbuch" results. Each page consisted of 50 lines which were consecutively numbered so that the entire book contained 10,000(or 9999) lines.(Informant was not sure of number of pages but positive that each page had 50 lines and that the lines were numbered only in 4 digits- i.e., from 0001 to 9999.)
Each line had 6 groups of 5 digit numbers. Example of page 1.

line no.	Random Groups
0001	56142 61513 00412 06111 71538 63254
0002	....
0003	(300 random groups per page)
....	....
0050	....
page 2	
0051	....
0052	....
....	....
0100	....

page 101 line no.	Random Groups
0501	54968 49597 00693 04999 39572 47056
0502	....
....	....
0550	....

(Compare line 0501 with 0001 and note that the numbers are correlated so that when added together they equal 00000. Further explanation later)

Encoding the message: In encoding from the Tangens Tafel, to the Satzbuch result is added 2 groups from the Tangens Tafel. The code worker arbitrarily choosed 2 lines from the T.T.(He has 9999 to choose from). He adds the groups of both these lines to the Satzbuch group. Example:

Plain text	und
Satzbuch no. for "und"	76500
1) From line 0412(e.g.)	

II. GRUNDVERFAHREN
("Ground"or "Basic")

This is a more complicated method of encoding which makes use of the following:

1. The Satzbuch (described above)
2. A cipher book of two types:
   a. "Tangens Tafel"(tangent table) T.T.
   b. "Grad Tafel" (degree or graduated table)G.T.
   Either or both may be used.
3. "Schlusselblock"(key pad)

This system involves:1-coding by use of the "Satzbuch ",2-making the message secure by adding numbers from the cipher books,3-including in the message an indicator as to how the cipher book was used. In the latter, the "key pad" is used.

1. "Satzbuch"
This is first used to change words and phrases into 5 digit groups as in the "Block" system.

2. Cipher books
Since two books were used, variations were possible.
a. Using only the "Tangens Tafel"(tangent table)
(This was used in Mexico City up until 1940 and possibly thereafter, according to the informant.)
Description of "TangensTafel": This is a 100 or 200(?) page book which served as a substitute for a cipher pad, i.e..it provided groups of 5 digits to be added to the "satzbuch" results. Each page consisted of 50 lines which were consecutively numbered so that the entire book contained 10,000(or 9999) lines.(Informant was not sure of number of pages but positive that each page had 50 lines and that the lines were numbered only in 4 digits- i.e., from 0001 to 9999.)
Each line had 6 groups of 5 digit numbers. Example of page 1.

line no.	Random Groups
0001	56142 61513 00412 06111 71538 63254
0002	••••• ••••• ••••• ••••• ••••• •••••
0003	(300 random groups per page)
....	••••• ••••• ••••• ••••• ••••• •••••
0050	••••• ••••• ••••• ••••• ••••• •••••

page 2

0051	••••• ••••• ••••• ••••• ••••• •••••
0052	••••• ••••• ••••• ••••• ••••• •••••
....	••••• ••••• ••••• ••••• ••••• •••••
0100	••••• ••••• ••••• ••••• ••••• •••••

page 101

line no.	Random Groups
0501	54968 49597 00698 04999 39572 47656
0502	••••• ••••• ••••• ••••• ••••• •••••
....	••••• ••••• ••••• ••••• ••••• •••••
0550	••••• ••••• ••••• ••••• ••••• •••••

(Compare line 0501 with 0001 and note that the numbers are correlated so that when added together they equal 00000. Further explanation later)

Encoding the message: In encoding from the Tangens Tafel, to the Satzbuch result is added 2 groups from the Tangens Tafel. The code worker arbitrarily choosed 2 lines from the T.T.(He has 9999 to choose from). He adds the groups of both these lines to the Satzbuch group. Example:

plain text		und
Satzbuch no. for "und"		76500
1) From line 0412(e.g.) of T.T.	56543	Add these:
2) " " 7015(e.g.)of		Do not carry.

Thus the final message consists of a series of groups which have been encoded as above.

Any two lines in the T.T. may be chosen by encoder. One starts with the first group in that line and adds the random groups found there (6 to a line) consecutively. If the message is longer than 6 groups the groups in the following lines are used. A second line is then chosed and another series of groups added to the messages.

Indicating of lines of T.T. which were used.: This is indicated in the final message by a group of 8 letters:

e.g. X A Q Y R T S O

The first 4 indicate the 1st line used and the last 4 indicate the 2nd line (of groups in the T.T.) which was used. These letters are arrived at through (1) adding from a small cipher pad (and 2) converting result to letters from table on the cover of the T.T.

i) Small cipher pad

Sheet 3" x 5" with 12 sheets, 1 for each month. Physically built like the larger pad. 15 or 16 lines on each sheet, depending on no. of days in month. 2 days on a line. Two 4 digit groups per line.

	JANUARY
1-2	4362 5416
3-4	7189 4022
5-6	....
27-28	....
29-30	....
31	....
day of month	2 four digit groups per line

This is used as the first step in disguising the numbers of the lines in the T.T. which were used in encoding the message. Suppose lines 412 and 7015 of the T.T. were used and the message was sent on January 4th.

	0412 7015
add:	7189 4022
result:	7591 1037

ii) Use of table on cover of T.T.

Note that the lines used in the T.T. to encode the message have now been encoded from the small cipher pad so as to result in an 8 digit number. (e.g. 75911037). This is now converted into an 8 letter group thru use of a table printed on the inside cover of the T.T. This may be called the Line Key Table (LKT) It contains: 1) the numbers 01 to 99, 2) with two letters given -- a vowel and a consonant - to equal each number. 10 consonants and 5 vowels were used. Informant could not recall exact consonants.

LINE KEY TABLE

AB-01	FA-11	EB-21	-31	
AF-02	FE-12	EF-		
AG-03	FI-13	EG-		
AN-04	FO-14			
AZ-05	FU-15			
BA-06	GA-16			
BE-07	GE-17		HE-37	
BI-08	GI-18			
BO-09	GO-19			
BU-10	GU-20	-30	-40	-50
-51	-61	-71	-81	PA-91
				PE
				PI
				PO
				PU

The line numbers which have already been encoded by adding numbers from small cipher pad are now converted to letters (8 letter group) thru use of above table. E.G.

75 91 10 37
NU PA BU HE

Final line indicator as it appears in the message.

Sample final message:

			No. of key cipher pad used(small)	T.T. lines indicator
	msg. no.	Date of Mo.		
"Auswärtige Berlin	141/04		41604	NUPABUHE

05754 71289 54321 ....
.... 000XX"
no. of secret groups

Decodings :

1) The decode requires the receiver to have a duplicate small cipher pad, the number of which is indicated by the second number group. (see example above). It also requires an exact duplicate Tabgens Tafel.

2) The number groups from the T.T. which were added to the message are determined from the 8 letter group (group 3) in the message:

a) Letters are changed to numbers from the table on the cover of the T.T. b) From these 8 numbers are subtracted the appropriate numbers on the small cipher pad; c) to result in two groups of 4 numbers which indicate lines in T.T. from which groups have been added to the message.

3) At this point a procedure is introduced which simplifies the mechanical work of decoding. Rather than subtracting twice (i.e. subtracting each group which had been added in encoding) the T.T. is so constructed as to permit decoding by addition process only. 5000 is added to each of the line indicators resulting in a new line indicator (a complementary line indicator). Then the two sets of groups indicated by the "complementary line indicator" are added to rather than subtracted from the encoded message. This results, however, in totaling up to the same number (Satzbuch number) as was found in the original message.

This process of the Tangens Tafel is called its secret. It is quite simple, however, The first 5000 lines of numbers (chosen by lottery) are complemented by the next 5000. The latter 5000 are so made up as to result in 0000 when added to the 5000th line preceding it. See example on pages 1 and 2 (supra)

First group on line 0001 when added to first group on line 5001 will equal 0000. Same is true of 4th group on lines 3433 and 8433, for example. etc. So -

When 5000 is added to line indicators and the groups in these complementary lines is added to the message (rather than subtracting the groups used in encoding) the desired result is achieved.

4) Upon completing the above, the message is readily changed from numbers to words by use of the "Satzbuch", resulting in the original plain text message.

b- Grad Tafel (G.T.) Variations

According to informant, the G.T. is identical in theory to the T.T. but merely uses different numbers. It may be used alone or in conjunction with the T.T.; e.g. one line of groups may be used from the T.T. and a second line from the G.T. The system used by the F.O. was varied

but no difficulty is encountered as long as both encoder and decoder follow the correct current procedure.

Comments of informant

T.T. and G.T. system is regarded as secure. However, it is troublesome and time-consuming both in encoding and decoding. The key to the security of the system lies in the small cipher pad which is used to disguise the line indicators.